INSTITUT D'ESTUDIS CATALANS
SECCIÓ DE CIÈNCIES I TECNOLOGIA

La teoria de grups finits

Discurs de recepció de
GABRIEL NAVARRO ORTEGA
com a membre numerari de la
Secció de Ciències i Tecnologia,
llegit el dia 6 de març de 2006

BARCELONA
2006

La teoria de grups finits

INSTITUT D'ESTUDIS CATALANS
SECCIÓ DE CIÈNCIES I TECNOLOGIA

La teoria de grups finits

Discurs de recepció de
Gabriel Navarro Ortega
com a membre numerari de la
Secció de Ciències i Tecnologia,
llegit el dia 6 de març de 2006

BARCELONA
2006

Biblioteca de Catalunya. Dades CIP

Navarro, Gabriel
La Teoria de grups finits
ISBN 84-7283-860-9
I. Institut d'Estudis Catalans. Secció de Ciències i Tecnologia II. Títol
1. Grups finits
512.54

Carrer del Carme, 47. 08001 Barcelona

Primera edició: octubre de 2006
Tiratge: 200 exemplars

Text revisat lingüísticament per l'Oficina de Correcció i Assessorament Lingüístics de l'IEC

Compost per Víctor Igual, SL
Carrer del Peu de la Creu, 5. 08001 Barcelona

Imprès a gama, s. l.
Carrer d'Arístides Maillol, 9-11. 08028 Barcelona

ISBN: 84-7283-860-9
Dipòsit Legal: B. 38303-2006

Per a Alexandre Turull

Per què matemàtiques? Per què àlgebra? Per què teoria de grups? Quines preguntes tan complicades! Si haguera de donar una resposta, si vertaderament estiguera forçat a fer-ho, jo crec que començaria a parlar de la perfecció o de l'absolut de les matemàtiques. Són llocs comuns, ho sé, però no en conec d'altres.

Sense cap intenció de polèmica amb els nostres col·legues químics, físics i d'altres: hi ha conjectures a les matemàtiques tan confirmades per les dades, comprovades en tants casos particulars, que qualsevol altre tipus de científic ja les haguera acceptades, momentàniament, com a certes. Però no un matemàtic. Algú em va preguntar: per a la resta de la societat, quina diferència hi ha en el fet que una conjectura estiga o no provada si estem segurs que és certa i tan sols hem d'esperar el nombre suficient d'anys perquè algú en trobe la demostració? No vaig saber ben bé què contestar en aquell moment. Però crec que ara contestaria que en la demostració està gran part del valor d'un teorema. I que només entenent per què una cosa és veritat, podrem anar més enllà.

Aquests són dies en els quals fins els matemàtics parlen d'utilitat i d'aplicacions. És fantàstic que alguna cosa siga útil per als altres. Quasi tots els matemàtics d'aquest país (però no d'altres) estan finançats amb fons públics, i sembla raonable que la societat ens demane explicacions del que es fa, i per a què es fa. Jo m'alegre quan, en comptades ocasions, bé és veritat, un químic o un físic em pregunten alguna cosa de representacions de grups. Sé que la teoria de representacions de grups té aplicacions a la cristal·lografia o a la física teòrica. També alguns topòlegs o geòmetres m'han preguntat alguna qüestió de grups, i aleshores em sent *útil*. Però si volen que siga completament sincer, jo no investigue per a ells. Fins i tot tinc la sensació que el que a ells els interessa té poc a veure amb el que a mi m'interessa. Hi ha un exemple que ens pot il·lustrar: la teoria de nombres, durant tants anys considerada pur *divertimento*, és avui un pilar fonamental a Internet, i en la seguretat de les comunicacions. Qui li ho hauria de dir a Fermat!

Açò vol dir que cal investigar-ho tot, que tot té el mateix interès? És clar que no. Cadascú sap quins són els problemes fonamentals en el seu camp, els problemes en què val la pena invertir temps (i diners) per a solucionar-los.

No sé si ho oblidava o és que no volia parlar d'això. He mencionat la perfecció, l'absolut de les matemàtiques, però no la bellesa de les matemàtiques... Ara mateix, fins i tot dubte que parlar d'açò siga políticament correcte. Si les matemàtiques són un art, nosaltres què som: artistes? A mi m'encantaria, però a uns altres col·legues crec que no tant. Recorde que he llegit llibres de físics famosos que parlen de la bellesa d'algunes equacions, i es pregunten qüestions com aquesta: una equació que descriu un fet fonamental pot ser lletja? Els matemàtics anem més enllà, és clar, i fins i tot parlem de la bellesa de les demostracions! Sir Michael Atiyah, medallista Field i Premi Abel, recentment ha escrit que perquè una demostració li agrade, ha de contindre una certa sorpresa, un gir de l'argument que no s'esperava. Com una bona pel·lícula.

El famós i singular matemàtic Paul Erdös deia que hi ha demostracions que directament vénen del Llibre (amb majúscules), és a dir, de déu (amb minúscules), i que els matemàtics, en algunes ocasions molt rares, tenen la fortuna d'accedir a algunes de les seues pàgines. Jo pense que tinc aquesta visió de les matemàtiques, que viuen en un món ideal, independent del nostre.

Però estic divagant. Abans he preguntat: Per què àlgebra? Em permetran que comence contant-los la història d'un problema fascinant, que marca el principi de l'àlgebra moderna. L'origen de l'àlgebra, no importa si el fixem en els antics egipcis, babilonis o grecs, està lligat a les *equacions polinòmiques*.

Tots sabem resoldre equacions polinòmiques de graus un i dos, les equacions lineals i quadràtiques. L'equació

$$ax + b = 0$$

té una única solució,

$$x = \frac{-b}{a},$$

com és clar. (No he dit què són a i b, però pensem que són números racionals.) L'equació

$$ax^2 + bx + c = 0$$

té dues solucions:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

(El cas on $b^2 - 4ac < 0$ era molt problemàtic per als antics perquè pensaven que els números negatius no tenien arrels quadrades, però no ho és per a nosaltres.)

Ara ve un detall que reflecteix la personalitat del matemàtic: què passa amb polinomis de grau tres, amb les equacions cúbiques? És quasi segur que vostès no recorden una fórmula per a les solucions de l'equació

$$ax^3 + bx^2 + cx + d = 0.$$

Jo tampoc. Aquest problema va ser resolt al Renaixement italià i publicat en la famosa *Ars magna* per Cardano (1545). Aparentment, les solucions les va descobrir Scipione del Ferro (1465-1526), que després de mantindre-les en secret li les va passar a un estudiant, Fior, abans de morir. Independentment, Tartaglia (1500-1557) havia trobat també solucions a algunes de les cúbiques. Després d'un concurs entre Fior i Tartaglia, guanyat per Tartaglia, sembla que aquest li les va comunicar a Cardano, amb la promesa que mai les publicaria... I la solució no és trivial. El que interessa ara dir és que hi ha tres solucions, i que aquestes es poden expressar amb sumes, multiplicacions i extracció d'arrels n-èsimes (radicals) dels coeficients a, b, c i d. Com en el cas quadràtic, però més complicat. En l'*Ars magna* de Cardano també apareixen les solucions de l'equació de grau quatre, descoberta, aparentment, per Ludovico Ferrari.

Després, però, comença la recerca de la solució d'una fórmula per a la quíntica. Matemàtics d'enorme talent com Leibniz, Euler, Lagrange o Ruffini ho intentaren sense èxit. Va ser, finalment, el matemàtic noruec Abel, al voltant de 1820, qui va donar la resposta, que encara a mi em fascina: hi ha polinomis de grau cinc tals que els seus zeros no són expressables mitjançant sumes, multiplicacions i radicals de llurs coeficients. Per exemple,

$$x^5 - x + 1 = 0.$$

No cometem l'error que cometen alguns estudiants de matemàtiques. L'anomenat *teorema fonamental de l'àlgebra* (de d'Alambert, Gauss i d'altres) ja ens assegura que tota equació polinòmica

$$a_n x^n + \cdots + a_1 x + a_0 = 0$$

té exactament n solucions (comptant solucions repetides). Però aquest no és el problema de què ara parlem. Nosaltres busquem si hi ha una fórmula «algebrai-

ca» d'escriure les solucions mitjançant els seus coeficients. En llenguatge modern, ens preguntem si les solucions estan en una extensió radical dels nombres racionals. I Abel ens diu que hi ha polinomis per als quals açò és fals. Llavors, quins són exactament els polinomis per als quals és veritat?

La nit abans de morir en un duel, Evariste Galois va deixar escrites les bases que solucionaven el problema i que constitueixen l'origen de l'àlgebra moderna. (En les seues últimes notes, escrites amb la tensió pròpia del que es sap en greu perill, també es poden llegir les paraules «une femme» —sembla que hi ha coses que mai canvien— i el que veig escriure a alguns estudiants a l'examen: «No tinc temps!!».) Després d'alguns antecedents, per Euler, Gauss, Lagrange o Cauchy (tant en teoria de nombres com en geometria), Galois és el primer que realment parla d'un grup, encara que no de la manera abstracta com el coneixem nosaltres.

Què era un grup per a Galois? Considerem, per exemple, l'equació polinòmica

$$x^4 - 10x^2 + 1 = 0.$$

Podem comprovar que les arrels d'aquest polinomi són:

$$\alpha = \sqrt{2} + \sqrt{3},\ \beta = \sqrt{2} - \sqrt{3},\ \gamma = -\sqrt{2} + \sqrt{3} \text{ i } \delta = -\sqrt{2} - \sqrt{3}\,.$$

Amb aquests quatre nombres reals, podem formar equacions algebraiques (amb coeficients racionals). Les equacions $\alpha + \delta = 0$, $\beta + \gamma = 0$, $(\alpha - \beta)^2 = 12$, etc., en són algunes.

Com sabem, hi ha vint-i-quatre maneres de permutar els «objectes» $\{\alpha, \beta, \gamma, \delta\}$. Per exemple,

$$f = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \alpha & \beta & \delta & \gamma \end{pmatrix}$$

és la permutació que envia $\alpha \mapsto \alpha$, $\beta \mapsto \beta$, $\gamma \mapsto \delta$, $\delta \mapsto \gamma$. Si apliquem f a l'equació

$$\alpha + \delta = 0$$

ens queda l'equació

$$\alpha + \gamma = 0,$$

que és falsa, perquè $\alpha + \gamma = 2\sqrt{3}$. Per tant, f és una permutació *falsa* per a l'equació polinòmica $x^4 - 10x^2 + 1 = 0$: transforma equacions vertaderes en falses. El que no és tan fàcil de demostrar és que

$$g = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \beta & \alpha & \delta & \gamma \end{pmatrix}$$

és una permutació *vertadera*: transforma qualsevol equació algebraica

$$\sum_i a_i(\alpha^{n_i}\beta^{m_i}\gamma^{k_i}\delta^{l_i}) = 0$$

en una altra que també és correcta. Es pot provar que hi ha exactament quatre permutacions vertaderes: g,

$$h = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \gamma & \delta & \alpha & \beta \end{pmatrix}, \quad k = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \delta & \gamma & \beta & \alpha \end{pmatrix},$$

i sens dubte la identitat

$$1 = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \alpha & \beta & \gamma & \delta \end{pmatrix}.$$

Per fi aquí tenim un grup:

$$G = \{1, g, h, k\},$$

el grup de l'equació polinòmica $x^4 - 10x^2 + 1 = 0$. És molt important que observem que si dues permutacions són *vertaderes*, la seua composició també ho és. Per exemple, $g \cdot h = k$, $h \cdot k = g$, o $g^2 = 1$. Si imaginen un rectangle amb vèrtexs α, β, γ i δ, observaran que G és exactament el conjunt de *moviments* del pla que fixen el rectangle.

Com hem vist, cada equació polinòmica $p(x) = 0$ té un grup associat G, el seu *grup de Galois*. El gran teorema de Galois afirma que hi ha una fórmula (amb sumes, multiplicacions i radicals dels coeficients del polinomi) per a les solucions de $p(x) = 0$ si i sols si el grup G és resoluble. Tornarem a la resolubilitat després.

Durant molts anys, els grups van ser *grups de permutacions*, és a dir, grups com els de Galois que permutaven objectes. El pas fonamental cap a l'abstracció el va fer Cayley al voltant de 1850. Aquest és un dels casos en els quals una definició resulta fonamental. Una vegada sabem el que és un grup, ens adonem que els grups estan per tot arreu, ordenant les matemàtiques.

El grup és l'estructura fonamental i bàsica, la mínima que té interès estudiar. Tenim un conjunt G on hi ha definida una *operació*. Per exemple, sumar funcions, multiplicar números, compondre aplicacions, multiplicar matrius. És a dir, per a cada dos elements $x, y \in G$, tenim definit un tercer $x \star y \in G$. (Recordem que si

x, y eren permutacions *vertaderes* de Galois, llavors la composició $x \star y$ també ho era.) Totes les possibles operacions en G no són interessants. G és grup si

$$(x \star y) \star z = x \star (y \star z)$$

per a tots $x, y, z \in G$; si existeix un element $1 \in G$ tal que

$$x \star 1 = 1 \star x = x$$

per a tot $x \in G$; i si per a tot $x \in G$ existeix un altre $y \in G$ tal que

$$x \star y = y \star x = 1.$$

Aquestes són les lleis naturals que l'experiència matemàtica ens ha dictat. Dos exemples fonamentals de grups serien S_n, o grup de les permutacions de n objectes, o el grup $\mathrm{GL}(n, \mathbf{C})$ de les matrius invertibles complexes $n \times n$. (Una vegada definit el grup G amb $\star$, escrivim $x \star y = xy$, perquè és més fàcil.)

Els grups estan íntimament relacionats amb la simetria, i de fet molts surten com a grups de simetries. Per exemple, el grup de simetries d'un quadrat, D_8, té vuit elements, de les quals les rotacions $\{1, G_{90}, G_{180}, G_{270}\}$ (girs de 90, 180 i 270 graus) formen un *subgrup*. (Un subgrup H de G és un subconjunt de G que forma grup amb l'operació de G.)

Els grups de simetries dels cinc sòlids platònics, o de les disset teselacions del pla, són ben coneguts. Les molècules tenen grups de simetria... I en general, quasi totes les estructures matemàtiques tenen un grup associat. D'una importància especial en el desenvolupament de la teoria de grups és el programa d'Erlangen de Felix Klein, en el qual es demana classificar els tipus de geometries mitjançant els grups que hi estan associats. De fet, per a Klein, la geometria és l'estudi de les propietats d'un espai que són invariants sota un determinat grup.

L'època moderna de la teoria de grups finits, però, comença amb W. Burnside (1852-1927) i el seu llibre *Theory of Groups of Finite Order*, publicat en 1897.

Nosaltres estem especialment interessats en els grups finits, els que tenen un nombre finit d'elements. Tots els dies tothom treballa amb un molt fàcil. El grup $\mathbf{Z}_{12}$ de les *hores* consisteix en els símbols {0 h, 1 h, 2 h, 3 h, ..., 11 h} on 12 h = 0 h. Per exemple, 0 h és l'element neutre, 7 h + 7 h = 2 h, etc. Açò ho podem fer no només per al número 12 sinó per a qualsevol número positiu n. Aquest és el grup cíclic $\mathbf{Z}_n$. Els grups cíclics són els més senzills que existeixen, i no tenen cap misteri.

Galois ja es va adonar que hi ha un tipus de subgrup fonamental, el *subgrup normal*. Un subgrup H de G és normal si el conjunt

$$Hx = \{hx \mid h \in H\}$$

és igual al conjunt

$$xH = \{xh \mid h \in H\}$$

per a tot $x \in G$. (O, equivalentment, si $x^{-1}hx \in H$ per a tots $x \in G$ i $h \in H$.) Sembla una mica tècnic però no ho és. És clar que 1 i G són dos subgrups normals de G, però sense importància. Els subgrups normals són fonamentals perquè si H és normal en G (ho escrivim $H \lhd G$), llavors podem construir un nou grup G/H. Cada vegada que surt un nou grup, és un esdeveniment que s'ha de celebrar!

Els elements d'aquest nou grup G/H són els subconjunts $\{H\,x \mid x \in G\}$ que es multipliquen com a subconjunts de G:

$$(Hx)(Hy) = H(xH)y = H(Hx)y = (HH)xy = Hxy.$$

Si G té $|G|$ elements, llavors

$$|G/H| = |G|/|H|.$$

(No hem comentat el teorema de Lagrange i ho hauria d'haver fet: si H és subgrup d'un grup finit G, aleshores $|H|$ divideix $|G|$; per tant, $|G|/|H|$ és un nombre enter.)

Si coneixem G, llavors coneixem G/H. Açò és un fet. En teoria de grups solem treballar per inducció: s'estudia un grup i es coneixen els grups d'ordre més petit. El que vull dir és que hom està intentant demostrar alguna cosa sobre G i troba que té un subgrup normal H de G, llavors té dos grups més petits íntimament associats a G que coneix: H i G/H (perquè són més petits, o per inducció). Tal vegada, això siga suficient per a provar el que es vol. (Per exemple, si G/H i H són resolubles, aleshores G és resoluble.)

Hi ha grups que, misteriosament, no tenen cap subgrup normal (excepte 1 i G): els grups *simples*. Els grups cíclics d'ordre primer són un exemple, però sense misteri. (Pel teorema de Lagrange, aquests grups no hi tenen espai per a cap subgrup.) Els grups simples no cíclics, malgrat el seu nom, són els grups més complicats que existeixen.

Si G és qualsevol grup finit, entre els normals H de G podem elegir H que tinga l'ordre més gran possible. És elemental provar que en aquest cas el grup $S = G/H$ és simple. D'aquesta manera a tot grup G sempre podem trobar una sèrie de subgrups

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_k \lhd G_{k+1} = G$$

on $S_i = G_i / G_{i-1}$ són simples. Aquests són els *factors de composició* de G, i estan unívocament determinats per G. I deu ser prou per a convèncer-los de la importància dels grups simples: sembla que tot grup finit està construït mitjançant grups simples.

És el moment de mencionar que G és resoluble si tots els S_i són cíclics d'ordre primer. Així, els grups resolubles són una mena de grups cíclics de *segona generació*. (Si recorden els grups de polinomis de Galois, l'extracció d'arrels n-èsimes està relacionada amb factors cíclics del grup de Galois. I és així com es prova el gran teorema de Galois de la resolubilitat d'equacions per radicals.)

Resumint, tenim dos tipus oposats de grups: els grups resolubles, la «segona generació» de grups cíclics, que tenen un munt de subgrups normals, i els grups simples, que no en tenen cap.

He dit que l'edat moderna de la teoria de grups finits comença amb Burnside, però l'edat actual comença amb J. G. Thompson. El 24 d'abril de 1959 apareix el titular següent en el *New York Times*:

50 YEAR PROBLEM IN MATH IS SOLVED
Student 26 proves finite conjecture. Explanation difficult

J. Thompson havia provat la conjectura de Frobenius i, més important, havia inventat la teoria local de grups finits que tan fonamental hauria de ser per a la teoria de grups. Com en teoria de nombres, els nombres primers són ben importants a la teoria de grups. Si p és un nombre primer que divideix $|G|$, aleshores G té subgrups d'ordre totes les potències de p que van dividint $|G|$. Associats a aquests, G té tota una xarxa de subgrups que s'anomenen *subgrups locals*. La teoria local diu que si es coneixen bé els subgrups locals, es té informació rellevant de tot el grup.

En qualsevol recol·lecció sobre els grups finits no pot faltar una menció a la classificació dels grups simples. Intentaré resumir en unes línies un teorema de centenars de matemàtics, de milers de pàgines, que és un dels més complicats, si no el que més, de les matemàtiques. Tenim una classe de grups simples molt fàcils: els cíclics d'ordre primer. Però n'hi ha d'altres, és clar. No sé si saben que les permutacions d'un conjunt de n elements es divideixen en dues classes: parelles e imparelles. Per exemple, la permutació

$$\begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}$$

és imparella; la permutació

$$\begin{pmatrix} \alpha & \beta & \gamma \\ \beta & \gamma & \alpha \end{pmatrix}$$

és parella. Del total de les $n!$ permutacions, la meitat són parelles i l'altra meitat imparelles. El conjunt de les permutacions parelles de n elements constitueix un grup, el *grup alternat* A_n, que és simple per a $n \geq 5$. Com que A_n no pot ser llavors resoluble, ara ja saben per què a partir de grau cinc, hi ha polinomis que no són resolubles per radicals. Hi ha una altra classe de grups simples, però, molt més nombrosa, associada a certes geometries sobre cossos finits: els grups simples de tipus Lie. (Per a tenir una idea, els grups de tipus Lie són la versió finita dels grups ortogonal $O(n, \mathbb{R})$, especial lineal $SO(n, \mathbb{R})$, etc.) La classificació dels grups simples afirma que si G és un grup finit simple, aleshores G és cíclic d'ordre primer, G és A_n per a $n \geq 5$, G és de tipus Lie o, sorpresa, G és un dels grups d'una llista de vint-i-sis. Aquesta llista de vint-i-sis grups, els anomenats *grups esporàdics*, constitueix, probablement, una de les llistes més famoses de les matemàtiques. Són grups simples singulars, criatures que s'han anat descobrint al llarg de més de cent anys, algunes només per ordinadors. El major de tots és el Monster, un grup finit d'aproximadament 10^{54} elements. Com he dit, la classificació és el treball de molts matemàtics, i no estaria bé mencionar tan sols uns pocs. Però sí que hem de parlar del teorema que ho comença tot. En 1963 W. Feit i J. Thompson provaren que els grups simples no abelians tenen un nombre parell d'elements.

Per a finalitzar, contaré una mica a què em dedique jo. La teoria de grups té dues eines fonamentals (que han estat la clau per a poder dur a terme la classificació, per exemple). Una és la teoria local, que ja hem mencionat. L'altra eina és la *teoria de representacions* iniciada per Frobenius. Una *representació* (complexa) d'un grup finit G és un *homomorfisme* de grups

$$\mathcal{X} : G \to \mathrm{GL}(n, \mathbf{C}).$$

(És a dir: $\mathcal{X}(gh) = \mathcal{X}(g)\ \mathcal{X}(h)$ per a tots $g, h \in G$.) De la representació només ens quedem amb la seva traça:

$$\chi: G \to \mathbf{C}$$

donada per

$$\chi(g) = \mathrm{Tr}(\mathcal{X}(g)).$$

Aquest es diu un *caràcter* de G de grau $\chi(1) = n$. És elemental provar que la suma de caràcters és caràcter, i aleshores ens quedem amb el conjunt $\mathrm{Irr}(G)$ de caràcters que no són suma de dos: els caràcters irreductibles de G. Aquestes funcions $G \to \mathbf{C}$ tenen propietats sorprenents. Per exemple, $\mathrm{Irr}(G)$ és base ortonormal de l'espai vectorial de funcions de classe $G \to \mathbf{C}$. O

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = |G|.$$

O $\chi(1)$ divideix $|G|$.

Els caràcters contenen informació d'enorme valor sobre el grup G. El fet que per a estudiar caràcters necessitem d'altres branques de les matemàtiques alienes a la teoria de grups (teoria d'anells, àlgebres, etc.) els dóna una profunditat difícil de descriure.

La teoria de grups i la de les seves representacions té encara molts problemes fonamentals per resoldre. La llista és molt llarga, i cadascú té les seues preferències. En qualsevol llista, però, podran trobar les conjectures de Brauer sobre blocs, o les conjectures d'Alperin-Broué-Dade-McKay, a les quals nosaltres ens dediquem des de fa uns quants anys. Totes aquestes conjectures tracten de la influència de l'estructura local en el conjunt $\mathrm{Irr}(G)$. Es creu que són certes, però ningú sap molt bé el perquè. Uns altres problemes fonamentals són estudiar les representacions modulars (sobre cossos de característica p), que encara no es coneixen per a grups tan importants com els simètrics, o els de tipus Lie. D'altres matemàtics intenten construir una nova demostració de la classificació dels grups simples. En la meva llista, com un homenatge a Galois i al seu teorema de resolubilitat, m'agradaria provar si el conjunt de graus dels caràcters de G determina la resolubilitat de G.

Bibliografia

Brauer, R.; Fong, P.; Wong, Warren J. [ed.]. *Collected Papers*. MIT Press, 1980.

Burnside, W. *Theory of Groups of Finite Order*. Cambridge University Press, 1897.

Curtis, C.; Reiner, I. *Representations and Characters of Finite Groups*. Interscience Publ., 1962.

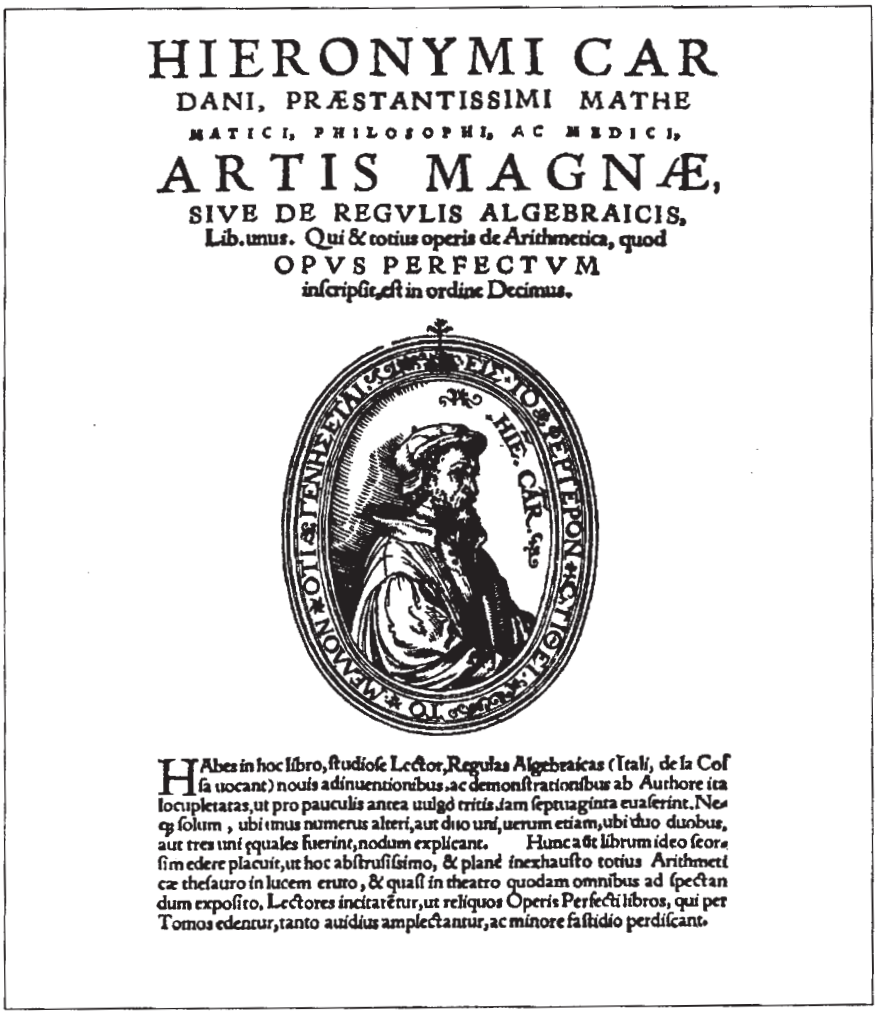
Feit, M.; Thompson, J. «Solvability of groups of odd order». *Pacific J. Math.*, núm. 13 (1963), p. 775-1029.

Gorenstein, D. *Finite Groups*. Nova York: Chelsea Publishing, 1968.

Huppert, B. *Endliche Gruppen*. Springer, 1967.

Isaacs, M. *Character Theory of Finite Groups*. Nova York: Dover, 1994.

Solomon, R. «A brief history of the classification of finite simple groups». *Bull. Amer. Math. Soc.* (*New Series*), núm. 38 (2001), p. 315-352.

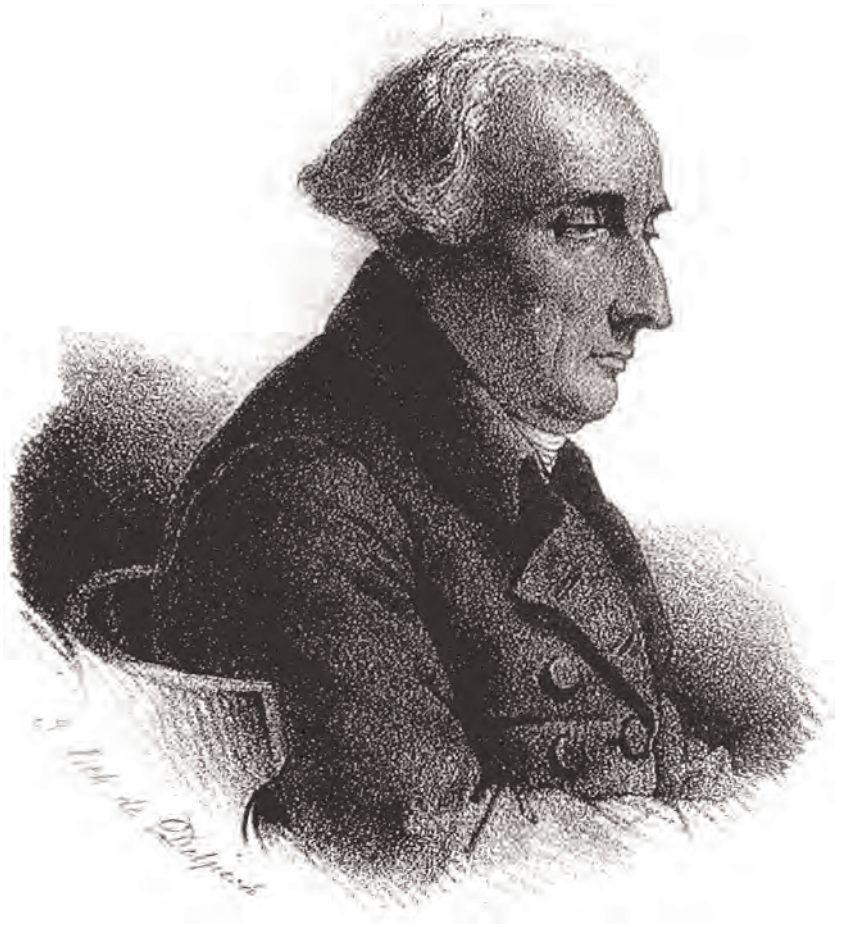


HIERONYMI CAR
DANI, PRÆSTANTISSIMI MATHE
MATICI, PHILOSOPHI, AC MEDICI,
ARTIS MAGNÆ,
SIVE DE REGVLIS ALGEBRAICIS,
Lib. unus. Qui & totius operis de Arithmetica, quod
OPVS PERFECTVM
inscripsit, est in ordine Decimus.

HIE. CAR.

HAbes in hoc libro, studiose Lector, Regulas Algebraicas (Itali, de la Cosa uocant) nouis adinuentionibus, ac demonstrationibus ab Authore ita locupletatas, ut pro pauculis antea uulgò tritis, iam septuaginta euaserint. Nec ea solum, ubi simus numerus alteri, aut duo uni, uerum etiam, ubi duo duobus, aut tres uni æquales fuerint, nodum explicant. Hunc ait librum ideo seorsim edere placuit, ut hoc abstrusissimo, & planè inexhausto totius Arithmeticæ thesauro in lucem eruto, & quasi in theatro quodam omnibus ad spectandum exposito, Lectores incitarentur, ut reliquos Operis Perfecti libros, qui per Tomos edentur, tanto auidius amplectantur, ac minore fastidio perdiscant.

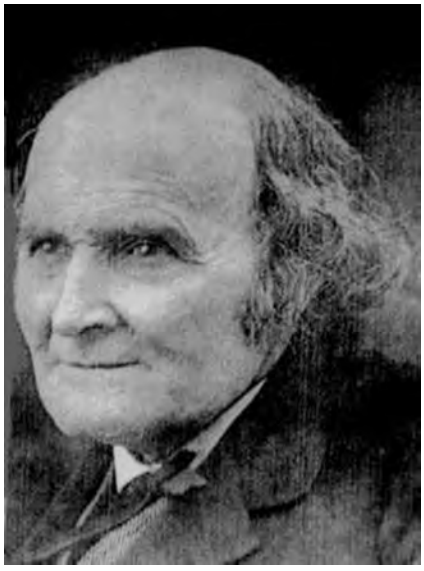
Ars magna, Gerolamo Cardano (1545).



Joseph-Louis Lagrange (1736-1813).

Niels Henrik Abel (1802-1829).

Évariste Galois (1811-1832).



Arthur Cayley (1821-1895).

William Snow Burnside (1852-1927).

Walter Feit i John G. Thompson.

IECentanys 1907 2007

ISBN 84-7283-860-9